JP:RTP
F #2013R01647

UNITED STATES DISTRICT COURT
EASTERN DISTRICT OF NEW YORK
– – – – – – – – – – – – – – – – – – – X

14 – 0003 M

IN THE MATTER OF AN APPLIATION FOR A SEARCH WARRANT FOR:

THE PREMISES KNOWN AND DESCRIBED AS (1) ONE APPLE IPHONE 4, FCC-ID NUMER BCG-E242B; (2) ONE MOTOROLA PHONE IMEI NUMBER 012907005594918; AND (3) ONE SAMSUNG GALAXY S4 PHONE, IMEI NUMBER 990003429718238

AFFIDAVIT IN SUPPORT OF APPLICATION FOR A SEARCH WARRANT

– – – – – – – – – – – – – – – – – – – X
EASTERN DISTRICT OF NEW YORK, SS:

JAMES HOLT, being duly sworn, deposes and states that she is a Special Agent with the Homeland Security Investigations ("HSI"), duly appointed according to law and acting as such.

Upon information and belief, there is probable cause to believe that there is located in THE PREMISES KNOWN AND DESCRIBED AS (1) ONE APPLE IPHONE 4, FCC-ID NUMER BCG-E242B; (2) ONE MOTOROLA PHONE IMEI NUMBER 012907005594918; and (3) ONE SAMSUNG GALAXY S4 PHONE, IMEI NUMBER 990003429718238 (the "DEVICES "), further described in Attachment A, the things described in Attachment B, which constitute evidence, fruits and instrumentalities of the crimes of importation of cocaine and attempted possession of cocaine with intent to distribute, in violation of Title 21, United States Code, Sections 952(a) and 841(a)(1) (the "TARGET OFFENSES").

The source of your deponent's information and the grounds for his belief are as follows:

1. I have been a Special Agent with Homeland Security Investigations ("HSI") for

approximately four years. I am responsible for conducting and assisting in investigations into the activities of individuals and criminal groups responsible for crimes related to unlawful importation and distribution of narcotics. I have participated in investigations involving search warrants and arrest warrants. As a result of my training and experience, I am familiar with the techniques and methods of operation used by individuals involved in criminal activity to conceal their activities from detection by law enforcement authorities.

2. I am familiar with the facts and circumstances of this investigation from: (a) my personal participation in the investigation, (b) reports made to me by other law enforcement authorities, and (c) records obtained pursuant to subpoenas. On the basis of this familiarity, and on the basis of other information that I have reviewed and determined to be reliable, I submit the following information.

I. BACKGROUND

3. On October 1, 2013, an individual now cooperating with the government ("CW") arrived at John F. Kennedy International Airport in Queens, New York, aboard JetBlue Airlines flight number 560 from Kingston, Jamaica. CW was selected for a Customs and Border Protection ("CBP") examination. During the examination, CW admitted, in sum and substance and in part, to ingesting 126 pellets of cocaine. An x-ray was taken of CW's intestinal tract, and the x-ray read positive for foreign bodies. CW passed 126 pellets, one of which field-tested positive for the presence of cocaine, with a total gross weight of 1.5139 kilograms.

4. CW agreed to cooperate with agents and stated, in sum and substance and in part, that beginning in July 2013, he made multiple drug trips from Jamaica to the United States and was paid between $1,000 and $6,000 for each trip. During four of those trips, once CW arrived to the United States, he contacted a person named "Dennis" for further instructions. On four of

the previous trips, CW gave the pellets he had been carrying to one or both of two individuals he met through "Dennis." CW agreed to place consensually monitored phone calls and texts to "Dennis" and these two men ("John Doe 1" and "John Doe 2"). During a monitored phone call, CW told "Dennis" that he anticipated passing all of the pellets by Thursday, October 3, 2013 and told "Dennis" to have the men meet him in New York at approximately 12:00 p.m. on October 3, 2013.

5. On October 3, 2013, CW received a phone call from John Doe 1, who said John Doe 1 would arrive in a white Nissan vehicle. John Doe 1 was later determined to be HENRY KANAGBOU. CW and agents arrived at the agreed-upon meeting location, which was a mall in Valley Stream, New York, and observed a white Nissan enter the parking lot. KANAGBOU was driving; HAROLD BOWENS was in the passenger seat. BOWENS got out of the car and entered the mall. CW carried a bag of sham cocaine pellets to the car and got inside. CW put the sham pellets in the back seat of the car and told KANAGBOU that he was to be paid $6,000. KANAGBOU made a phone call to a John Doe 2, who told CW that he would be paid when he returned to Jamaica. KANAGBOU gave CW a bag of clothes to give to "Dennis."

6. Agents waited until BOWENS left the mall. BOWENS and KANAGBOU were arrested. THE APPLE IPHONE 4, FCC-ID NUMER BCG-E242B was recovered from BOWENS; THE MOTOROLA PHONE IMEI NUMBER 012907005594918 and SAMSUNG GALAXY S4 PHONE, IMEI NUMBER 990003429718238 were recovered from KANAGBOU.

7. After waiving his Miranda rights, KANAGBOU agreed to speak with agents. He admitted, in sum and substance and in part, that he knew he was coming to New York to pick up something illegal and was to be paid $350 and a reimbursement for gas and tolls by John Doe 2.

KANAGBOU stated, in sum and substance and in part, that one of the phones recovered from him was the phone that he had previously used for drug dealing.

8. After waiving his Miranda rights, BOWENS also agreed to speak with agents. He admitted, in sum and substance and in part that KANAGBOU was coming to New York to pick up drugs and that KANAGBOU was going to give BOWENS over $100 for driving him to New York.

9. On October 4, 2013, CW, KANAGBOU and BOWENS were charged by criminal complaint in the Eastern District of New York, Docket No. 13-M-868, with conspiracy to distribute a controlled substance, in violation of Title 21, United States Code, Sections 841(a)(1). On November 27, 2013, a grand jury indicted KANAGBOU and BOWENS for, inter alia, conspiracy to distribute a controlled substance, in violation of Title 21, United States Code, Sections 841(a)(1).

II. TECHNICAL TERMS

10. Based on my training and experience, I use the following technical terms to convey the following meanings:

a. Wireless telephone: A wireless telephone (or mobile telephone, or cellular telephone) is a handheld wireless device used for voice and data communication through radio signals. These telephones send signals through networks of transmitter/receivers, enabling communication with other wireless telephones or traditional "land line" telephones. A wireless telephone usually contains a "call log," which records the telephone number, date, and time of calls made to and from the phone. In addition to enabling voice communications, wireless telephones offer a broad range of capabilities. These capabilities include: storing

names and phone numbers in electronic "address books;" sending, receiving, and storing text messages and e-mail; taking, sending, receiving, and storing still photographs and moving video; storing and playing back audio files; storing dates, appointments, and other information on personal calendars; and accessing and downloading information from the Internet. Wireless telephones may also include global positioning system ("GPS") technology for determining the location of the device.

b. Digital Camera: A digital camera is a camera that records pictures as digital picture files, rather than by using photographic film. Digital cameras use a variety of fixed and removable storage media to store their recorded images. Images can usually be retrieved by connecting the camera to a computer or by connecting the removable storage medium to a separate reader. Removable storage media include various types of flash memory cards or miniature hard drives. Most digital cameras also include a screen for viewing the stored images. This storage media can contain any digital data, including data unrelated to photographs or videos.

c. Text Messages: Text messaging, or texting, refers to the exchange of brief written text messages between fixed-line phone or mobile phone and fixed or portable devices over a network, and include messages which contain image, video, and sound content.

d. Internet: The Internet is a global network of computers and other electronic devices that communicate with each other.

e. Electronic mail: Electronic mail, commonly called email or e-mail, is a method

of exchanging digital messages from an author to one or more recipients. Modern email operates across the Internet or other computer networks. A sent or received email typically includes the content of the message, source and destination addresses, the date and time at which the email was sent, and the size and length of the email. If a sender or recipient of the message does not delete the message, the message can remain on the device indefinitely. If an email user writes a draft message but does not send it, that message may also be saved on the device but may not include all of these categories of data. The DEVICES can also store files, including emails, address books, contact or buddy lists, calendar data, pictures, and other files. In my training and experience, evidence of who was using an email account may be found in address books, contact or buddy lists, emails on the device, and attachments to emails, including pictures and files.

f. Facebook/MySpace: Facebook and MySpace are social networking services and websites. Users of these sites may create a personal profile, add other users as friends, and exchange messages, including automatic notifications when they update their profiles. Users must register before using the sites. Users can create profiles with photos, lists of general interests, contact information, and other personal information. Users can communicate with friends and other users through private or public messages and a chat feature. Users can access and store personal information, such as contacts, telephone numbers, and photographs on their accounts.

g. Storage medium: A storage medium is any physical object upon which electronic data can be recorded. Examples include hard disks, floppy disks, memory cards,

digital video recorder machines ("DVRs"), CD-ROMs, and several other types of magnetic or optical media not listed here.

11. Based on my knowledge, training, and experience, I know that the DEVICES have capabilities that allow them to serve as a wireless telephone and digital camera, and can be used to send and receive electronic mail and text messages and to access the Internet and websites including Facebook or MySpace. In my training and experience, examining data stored on devices of this type can uncover, among other things, evidence that reveals or suggests who possessed or used the DEVICES.

III. THE DEVICES

12. Based upon my training and experience, I know that those who import, distribute and possess with intent to distribute narcotics do not act alone and often communicate with coconspirators by means of wireless telephones such as the DEVICES. Those who commit such offenses may also retain evidence of their participation in such crimes on wireless telephones through call records, text messages, WhatsApp messages, emails or photos. Based upon my knowledge, training and experience, I know that those who import, distribute and possess with intent to distribute narcotics often communicate by means of text messages or electronic mail.

13. Based upon my training and experience with cases involving drug couriers who arrive at the airport with narcotics concealed in their luggage, I know that such individuals are commonly instructed to call someone upon arrival to the United States to arrange delivery of the narcotics. Here, HSI agents recovered the DEVICES from KANAGBOU and BOWENS after they arrived to accept a delivery of purported cocaine from a drug courier. Furthermore, both KANAGBOU and BOWENS admitted involvement . KANAGBOU admitted that one of the DEVICES was used for drug dealing. Accordingly, there is probable cause to believe there is

information stored on the DEVICES pertaining to KANAGBOU and BOWENS' conspiracy to import of cocaine and attempted possession of cocaine with intent to distribute.

14. I know that the DEVICES can store information for long periods of time. Similarly, things that have been viewed on the Internet can be stored for some period on electronics like the DEVICES. This information can sometimes be recovered with forensic tools.

IV. TECHNICAL BACKGROUND

15. As further described in Attachment B, this application seeks permission to locate not only electronic files that might serve as direct evidence of the crimes described on the warrant, but also for forensic electronic evidence that establishes how the electronic devices were used, the purpose of their use, who used them, and when. There is probable cause to believe that this forensic electronic evidence will be stored on the DEVICES because:

a. Data on an electronic device can provide evidence of a file that was once on the device but has since been deleted or edited, or of a deleted portion of a file (such as a paragraph that has been deleted from a word processing file). Virtual memory paging systems can leave traces of information on the device that show what tasks and processes were recently active. Web browsers, email programs, and chat programs store configuration information on the device that can reveal information such as online nicknames and passwords. Operating systems can record additional information, such as the attachment of peripherals, the attachment of USB flash storage devices or other external storage media, and the times the device was in use. Electronic devices can record information about the dates files were created and the sequence in which they were created.

b. Forensic evidence on an electronic device can also indicate who has used or controlled the device. This "user attribution" evidence is analogous to the search for "indicia of occupancy" while executing a search warrant at a residence. For example, registry information, configuration files, user profiles, email, email address books, "chat," instant messaging logs, photographs, the presence or absence of malware, and correspondence (and the data associated with the foregoing, such as file creation and last-accessed dates) may be evidence of who used or controlled the electronic device at a relevant time.

c. A person with appropriate familiarity with how an electronic device works can, after examining this forensic evidence in its proper context, draw conclusions about how devices were used, the purpose of their use, who used them, and when.

d. The process of identifying the exact files, blocks, registry entries, logs, or other forms of forensic evidence on an electronic device that are necessary to draw an accurate conclusion is a dynamic process. While it is possible to specify in advance the records to be sought, such evidence is not always data that can be merely reviewed by a review team and passed along to investigators. Whether data stored on an electronic device is evidence may depend on other information stored on the device and the application of knowledge about how the device behaves. Therefore, contextual information necessary to understand other evidence also falls within the scope of the warrant.

e. Further, in finding evidence of how an electronic device was used, the purpose of its use, who used it, and when, sometimes it is necessary to establish that a particular thing is not present on an electronic device. For example, the presence

or absence of counter-forensic programs or anti-virus programs (and associated data) may be relevant to establishing the user's intent.

16. Based on the foregoing, and consistent with Rule 41(e)(2)(B), the warrant I am applying for would permit the examination of the DEVICES consistent with the warrant. The examination may require authorities to employ techniques, including but not limited to computer-assisted scans of the entire medium, that might expose many parts of the DEVICES to human inspection in order to determine whether it is evidence described by the warrant.

17. Because this warrant seeks only permission to examine devices already in law enforcement's possession, the execution of this warrant does not involve the intrusion into a physical location. Consequently, I submit there is reasonable cause for the Court to authorize execution of the warrant at any time in the day or night.

V. CONCLUSION

18. Based on my training and experience, and the facts as set forth in this affidavit, there is probable cause to believe that on the DEVICES there exists fruits, instrumentalities and evidence crimes of conspiracy to commit possession of narcotics with intent to distribute and distribution of narcotics, in violation of Title 21, United States Code, Sections 952(a) and 841(a)(1). Accordingly, a search warrant is requested.

19. It is respectfully requested that this Court issue an order sealing, until further order of this Court, all papers submitted in support of the application, including the application and search warrant. I believe that sealing these documents is necessary because the items and information to be seized are relevant to an ongoing investigation into criminal organizations, and that not all of the targets of this investigation will be searched at this time. Based upon my training and experience, I have learned that criminals actively search for criminal affidavits and

search warrants via the internet, and disseminate them to other criminals as they deem appropriate, e.g., by posting them publicly through online forums. Premature disclosure of the contents of this affidavit and related documents may have a significant and negative impact on the continuing investigation and may severely jeopardize its effectiveness.

WHEREFORE, your deponent respectfully requests that the requested search warrant be issued for the DEVICES, more particularly described in Attachment A, to search for the records and information described in Attachment B, all of which constitute evidence, fruits and instrumentalities of violations of 21 U.S.C. §§ 952(a) and 841(a)(1).

IT IS FURTHER REQUESTED that all papers submitted in support of this application, including the application and search warrant, be sealed until further order of the Court.

S/ James Holt

JAMES HOLT
Special Agent
Homeland Security Investigations

Sworn to and subscribed before me
This 6th day of January, 2014

S/ Lois Bloom

THE HONORABLE LOIS BLOOM
UNITED STATES MAGISTRATE JUDGE
EASTERN DISTRICT OF NEW YORK

ATTACHMENT A

Property to Be Searched

The property to be searched is (1) ONE APPLE IPHONE 4, FCC-ID NUMER BCG-E242B; (2) ONE MOTOROLA PHONE IMEI NUMBER 012907005594918; and (3) ONE SAMSUNG GALAXY S4 PHONE, IMEI NUMBER 990003429718238, hereinafter the "DEVICES." This warrant authorizes the forensic examination of the DEVICES for the purpose of identifying the electronically stored information described in Attachment B.

ATTACHMENT B

Particular Things to be Seized

All information obtained from the DEVICES will be maintained by the government for the purpose of authentication and any potential discovery obligations in any related prosecution. The information shall be reviewed by the government only for the purpose of identifying and seizing information that constitutes fruits, evidence and instrumentalities of violations of importation of cocaine and attempted possession of cocaine with intent to distribute, in violation of Title 21, United States Code, Sections 952(a) and 841(a)(1), including:

1. All records and information on the DEVICES described in Attachment A, between July 1 1, 2013 and October 10, 2013, including names and telephone numbers, as well as the contents of all call logs, text messages, emails (including those sent, received, deleted and drafted), instant messages, photographs, videos, Facebook posts, Internet activity (including browser history, web page logs and search terms entered by the user), and other electronic media constituting evidence, fruits or instrumentalities of importation of cocaine and possession of cocaine with intent to distribute, in violation of Title 21, United States Code, Sections 952(a) and 841(a)(1);

2. All contact lists;

3. Evidence of user attribution showing who used or owned the DEVICES at the time the things described in this warrant were created, edited or deleted, such as, for example, logs, phonebooks, saved usernames and passwords, documents and browsing history; Passwords, encryption keys and other access devices that may be necessary to access the DEVICES;

4. Contextual information necessary to understand the evidence described in this attachment;

all of which constitute evidence, fruits and instrumentalities of importation of cocaine and attempted possession of cocaine with intent to distribute, in violation of Title 21, United States Code, Sections 952(a) and 841(a)(1).

As used above, the terms “records” and “information” include all of the foregoing items of evidence in whatever form and by whatever means they may have been created or stored, including any form of computer or electronic storage (such as flash memory or other media that can store data) and any photographic form.